Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

INFORMING (IN)STABILITY

The Security Implications of a Shifting News and Media Environment

Global Futures Forum workshop
21–22 February 2012, Ottawa

Informing (In)Stability

The Security Implications of a Shifting News and Media Environment

A conference of the Canadian Security Intelligence Service held in collaboration with Policy Horizons Canada

Highlights from the conference
21-22 February, 2012, Ottawa

The conference and its objectives

On 21 and 22 February 2012, the Academic Outreach program of the Canadian Security Intelligence Service, in partnership with Policy Horizons Canada, hosted a conference at its headquarters in Ottawa to examine the evolution of the news and media environment globally and discuss related security consequences. The conference drew over 100 officials and non-governmental experts and was held under the umbrella of the Global Futures Forum, a multinational, security-focussed research and foresight network linking security organisations in over 20 countries.

Information technology is no longer a simple "add-on tool" allowing for tasks to be performed faster and more efficiently. It is now a genuine force for social, political and economic movements of all kinds, as illustrated in part during the political upheaval in the Arab world beginning in early 2011. Since the mid-1990s, the traditional notion of media reporting has come under increasing pressure: the rise of the Internet, allowing everyone to broadcast contents and participate directly in the "public discourse", has atomised the concept of expertise. No one is arguing for a return to the days preceding the personal computer and network technologies, whose benefits are widely understood. But is there a flip-side to this? Might there be security considerations to an ever expanding information environment with its own dynamic? Will ever deeper and "always-on" expressions of individualism make it growingly difficult for the necessary trade-offs to be made to guarantee collective security?

The exponential explosion of contents on the web makes more widely available some of the knowledge required to understand threats. But it may also mark the opening of a chaotic information period in which the ability of both citizens and governments to find, create and openly influence streams of information will be challenging, making digital literacy all the more important for a country's stability. Absent the so-called "common narrative" that have rooted Western societies since the 19th century, how will governments mobilise public opinion around sophisticated security problems? How could countries become more vulnerable to manipulation and other influence? How might the relationship between governments and information evolve? Those questions form the basis upon which the conference unfolded.

The conference welcomed a diverse range of participants and leading experts from Asia, Canada, Europe and the United States. It addressed a selection of key themes and set a background for a continuing dialogue on salient ones. This report summarises the main ideas presented by experts and discussed amongst participants during the course of the event. It should also be noted that the views, ideas and concepts in this report do not reflect official positions of CSIS and are offered as a means of supporting an ongoing discussion.

Executive Summary

Turmoil and transition in the media industry is not only a literal demonstration of shifts in information technology, but also a reflection of the challenges facing all legacy institutions. Any institution that in the 20th century relied on, and gained power and authority through, the creation and control of information is being challenged by a new global information ecosystem that, "like water in cracks", erodes the foundations of hierarchical systems.

Disruption and creative destruction are forces that have a positive and innovative collective impact on the business sector. In the media industry, this means Internet start-ups competing directly for readers with *The New York Times*. Despite the latter's long reputation for excellence in the field of journalism, it is not inconceivable that an online competitor, freed of legacy costs such as printing presses, delivery trucks and labour unions, could one day replace it or part of its offering.

Intelligence agencies are in many ways similar to news organisations. Their value lies in their ability to know about and analyse events quickly and accurately. But government institutions face a singular challenge and the unique role of sovereign government implies that intelligence organisations cannot be replaced by start-ups. In this case disruptive change has to come from within; organisations face periods of self-reform, and they must determine in what areas they add value and shed other areas where they do not. Government departments and intelligence services stand to gain from the innovation occurring in the realms of information, technology and data, causing them to adapt to evolving functions and rethink their relationship with the public.

While the discussion at the conference was wide ranging, this report synthesises the four main themes addressed:

- the recent historical and theoretical shifts that explain the information-driven world;
- the ways in which information technology is instrumental to this new reality;
- the challenges faced by both democratic and autocratic governments; and
- new ways for government institutions to operate in this new ecosystem.

Theorising the New World

New information technologies are radically changing the ways we interact, communicate, understand, and act on all scales. State institutions, like all hierarchical 20th-century organisations, are fundamentally threatened by this flattening. Corporations, international organisations, media companies, and government agencies were built for a world where power was achieved through the control of information. Deep knowledge of market trends, opinions, international events and the news provided strategic advantages for large institutions with the capacity to collect and process information.

The transformation of how we create, distribute, consume and share news is therefore both representative of this shift (news organisations are struggling like all other legacy institutions), and foundational to it (the change in access to information affects all other institutions). Analysing these changes through the lens of media then offers two parallel benefits: it serves to depict how government institutions such as intelligence organisations may need to undergo serious reform in order to remain relevant, and it demonstrates the attributes of the new information technology landscape on which they must now engage.

Three theoretical approaches serve this analysis well. First, the metaphor of the "Gutenberg parenthesis" frames our networked world in historical terms. We are coming out of a period in history defined by the linear and bound constraints of the printing press, and into an era of networked story-telling that looks a lot like the pre-Gutenberg world. Second, technological empowerment and a permanent state of "being networked" is gradually giving birth to poly-social selves; it can be argued that we now live multiple simultaneous selves, in various mixes of online and offline states, which will challenge how we think about both individuality and society. Third, we see the emergence of the "fifth estate", a social group enabled by information technology that challenges the existing social order by attempting to hold to account institutions and individuals.

Media and Information Technology as Instrumental

If we are in the middle of a societal transformation from a printed age to a digital age, what are the core attributes of a world that is digitally enabled? Information technology has become instrumental to the practice of trade, politics, culture and society, as well as the way individuals act and think. In particular, it is changing long-held notions of power, authority, cohesion and transparency in several ways.

First, even though the world is increasingly connected, online power, measured as participation in knowledge production, still follows traditional global power imbalances. A key point is how more people, across more cultural, wealth, regional and technological divides can participate in digital globalisation. Particularly for Western countries, which have to date disproportionately influenced the development of Internet, we also see growing potential for decreased accessibility to information as non-Western languages gain an increasing share of the active online space.

Second, as control over information is decentralised, it becomes harder for institutions to retain authority based simply on historical credibility. Legitimacy is now easily undermined unless hierarchical institutions can convince an increasingly sceptical public of their utility. In a new media environment, authority is earned. Eroding political authority is accompanied by the multiplication of propagandistic world-views sponsored most often by states and at times certain sub-state actors. This is something we can observe in the burgeoning competition for attention in the field of international news broadcasting.

Third, the new information technology world is fragmented. Although people still read and consume media from legacy content providers, the range of content created and consumed in other networks is expanding rapidly. This expansion is leading to a large-scale fragmentation of our discourse and, by undermining the very possibility of a single national or historical narrative, raising new questions about social cohesion. As one speaker indicated when referring to political participation, "the Internet makes it increasingly easy to say *no* [ie. to challenge], but we have yet to see its force harnessed to say *yes*." Moreover, as all individuals and organisations become not only users but also potential producers of information and knowledge, the question of source reliability and the risk for disinformation become ever more significant.

Fourth, in a time when vast amounts of information are available to anyone, any time, the question of what information is public and what information is protected or private is increasingly complex. Information security is further challenged by the proliferation of organisations such as Anonymous and Wikileaks, whose very purpose is to publish protected and private information.

How governments deal with these societal shifts will go a long way in predicting their ability to connect with, and earn the trust of, the citizens they serve.

The Challenges Facing Democratic and Autocratic Governments

The new information technology architecture challenges all hierarchical organisations: news companies, blue-chip corporations and multinational organisations such as the UN. This necessarily includes modern government. A public empowered by information abundance has both new demands for the state and new expectations of the relationship between a government and its citizens. Democratic states face issues of privacy, public perception, authority and data policy. Autocratic states could face existential challenges from an empowered population.

How does the democratic state deliver health care when self-diagnosis reaches full fruition? How does the government provide public education when citizens can monitor and evaluate the quality of teaching in real time? The question becomes even more challenging when looking at the security apparatus of the state. The roles of intelligence services, the police and the military, like those of all large organisations, are gradually bending under the weight of data overload, increasing public expectations of transparency and the reality that such organisations no longer hold a monopoly on security information, but are instead part of a global information space.

Whereas the challenges posed by information technology in democratic states are largely managerial in nature, the opportunities offered by information technology for promoting democracy in autocratic states can be revolutionary. An autocracy is the absolute manifestation of the power of controlling information. However, we should guard against the temptation to envision a future that is linear or to draw facile conclusions: new technologies will not automatically make all governments perfectly democratic. Autocratic regimes, too, are adopting technology and benefitting from innovation.

Operating in this New Ecosystem?

Hierarchical organisations are at a crossroads. Information technology and networked organisations both challenge and disrupt their very existence. If the organisation is a private corporation, such as a newspaper or an auto manufacturer, then creative destruction may very well be a net positive. The online news sources and aggregators *The Huffington Post* and *ProPublica* could conceivably replace *The New York Times*, and electric car-maker Tesla Motors might replace Ford. Creative destruction is

more difficult, however, in the public sector. The foreign ministries, police forces and intelligence agencies are not simply going to disappear and be replaced by start-ups. The new information environment, however, may require them to adopt some of the start-ups' characteristics.

This is a sweeping task, and there are several areas in which government institutions in general can begin to rethink their social role and operating procedures to continue to deliver on their mandate in the future.

Reverse organisational engineering: The challenge for governments is how to rebuild, reform and reimagine their institutions to maintain relevance and to function effectively in a digital era. Instead of simply moving old institutions online, we may do the opposite and look at online dynamics and forms of communication and action to use them as models to plan the future evolution of existing institutions or to create new ones.

Protecting the system: Protecting the underlying sociological and legal systems, as well as physical infrastructure, is a core priority of government. This becomes even more important as we see unregulated cyberspace and the real world increasingly sharing the same mix of social, political and economic realities.

Embracing big data: For the intelligence community, "big data" is both a blessing and a curse. It can be used for situational awareness, to predict the size of demonstrations, to understand what groups think about specific issues, to detect spontaneous events and to monitor threats. However, this usefulness is mitigated by the pure physical challenges of dealing with massive data flows and the ethical questions of how governments *should* use the data they collect.

Rethinking education: Finally, in the new information technology world, literacy has taken on an entirely new meaning. It is no longer enough to train our citizens to read, write and perform basic calculations. They also need to become digitally aware and use critical thinking to assess both the content they access and the underlying technology used to deliver such content to them.

1
Workshop Synthesis

Workshop Synthesis

While it is tempting to separate the changes and challenges facing the industry of news and the practice of journalism from the shifts occurring in the intelligence world, in reality they are both functions of a much wider societal shift. Any institution that in the 20th century relied on, and gained power and authority through, the creation and control of information is being challenged by a new global information ecosystem, which "like water in cracks" erodes the foundations of hierarchical systems. This new ecosystem is characterised by, among other variables, information abundance, social distribution, new definitions of authority, and the free flow of data between network nodes. Determining the role of an intelligence service in this context requires understanding the ecosystem's origins, its principal characteristics today and the core challenges and opportunities it presents.

The first part of the report provides a synthesis of the four main themes examined during the conference: 1) theorising the new world; 2) the instrumentality of media and information technology; 3) the challenges facing democratic and autocratic governments; and 4) operating in this new ecosystem. The second half of the report summarises each of the expert presentations delivered during the event.

The report thus offers a thematic overview of what was a dynamic, two-day conference; it also gives leads and clues to examine further as we begin to imagine the future of intelligence services.

Theorising the New World

Few would doubt that we are living through a transition into a new informational world. The ways we interact, communicate, understand and act on all scales have been radically transformed by new information technologies. State institutions, like all hierarchical 20th-century hierarchies, are fundamentally threatened by this flattening. Corporations, international organisations, media companies, and government agencies were built for a world where power was achieved through the control of information. Deep knowledge of market trends, opinions, international events and news gave strategic advantages to large institutions with the capacity to collect, process and control information.

The profound shift in how we create, distribute, consume and share news is therefore both representative of the emerging politics of information (news organisations are struggling like all other institutions) and foundational

to it (the change in access to information affects all other institutions). Analyzing these changes through the lens of media then offers two parallel benefits: it serves to depict how institutions like intelligence organisations may face increasing pressure to remain relevant, and it illustrates the attributes of the new global information space.

Three theoretical approaches serve this analysis well. First, the metaphor of the "Gutenberg parenthesis" frames our networked world as having a clear historical antecedent. We are coming out of a period in history defined by the linear and bound constraints of the printing press, and into an era of networked storytelling that looks a lot like the pre-Gutenberg world. Second, technological empowerment and a permanent state of "being networked" is gradually giving birth to poly-social selves; it can be argued that we now live multiple simultaneous selves, in various mixes of online and offline states, which will challenge how we think about both individuality and society. Third, we see the emergence of the "fifth estate," a social group enabled by information technology that challenges the existing social order by attempting to hold to account institutions and individuals.

The Gutenberg Parenthesis

The idea of the "Gutenberg parenthesis" stipulates that we are now at the culminating moment of a revolution that will be complete when all cultural and knowledge production has been digitised—when all books ever written are digitised, all art reproduced, all news online. When this occurs, when our primary mode of interaction, communication and production all *become* digital information, we will have ended a period of human history that was enabled by Gutenberg's printing press, the latter having made it possible to contain information which naturally tends to disperse.

The printing press represented a shift from the chaotic, oral tradition to the linear, written one. The work of William Shakespeare, for example, anchored the English language into this new form. The alphabet and written word took on an entirely different social value and role. This transformation reached a culminating point in the 16th century when the number of printed copies exceeded the number of original manuscripts in Europe.

The printing press had wide-reaching consequences. In addition to allowing for the widespread dispersal of information, it also shaped how information itself was conceived. If one wanted information to spread, one needed to conform to a specific form, which was linear and bound.

It had beginnings, middles and ends. Ideas were constructed to fit this form, and knowledge evolved via the constraints it imposed. Society moved from a decentralised oral tradition of knowledge sharing to one that could be centralised, controlled and mass-produced.

If the modern era is characterised and determined by the printing press, then its reach and consequences are vast. Some 350 years of governance, institutional design, political evolution, media and culture were all dictated by humankind's rapport with information technology. If we are now adopting a new mode of information production, one based on digital information, then the implications are similarly destabilising.

This new shift marks the end of the Gutenberg parenthesis. With it, we are returning to many of the same characteristics as the pre-Gutenberg world. Ancient folk and digital storytellers indeed share many attributes in that they are open-ended and explore pathways that vary with each performance. They are increasingly unbound by the constraints of the printed form, freed from the physicality of printed information.

Take for example media. Inside the Gutenberg parenthesis (roughly from 1500 to 2000), it contains words between margins, collected in books, organised in bookcases. In the pre-parenthesis world, media existed thanks to private connections between individuals forming slowly evolving networks. In the post-parenthetical world, media is reflected in our technology and shared via complex patterns of hypertext and links. As a mode of cultural mediation fuelled by the written word, the Gutenberg parenthesis constitutes a defined period of history.

The result is that the media changes we are witnessing today, while driven by more sophisticated technology, are also taking us back to older, "messier" ways of communicating. This metaphor has three principle implications for information technology and intelligence.

First, news production is altered significantly because expertise is transient, instead of residing in a few individuals only. Within the Gutenberg Parenthesis the standard medium for news was printed newspaper, a

physical container that was refilled daily. Journalists and editors were the gatekeepers of what was considered news. We now observe a continuous avalanche of updated reports that break the modern linearity of news. News after Gutenberg tends to be cumulative and authored collectively. The journalist has become a navigator on, rather than a proprietor of, this information.

Second, our notion of threat is expanding beyond the confines of traditional power, control and behaviour. On one hand, the post-parenthetical hacker and the pre-parenthetical terrorist have more in common with each other than with the moderns born within the parenthesis. The present and immediate security future will be marked by encounters, confrontations and conflicts between pre-parenthetical illiterate individuals, parenthetical literate individuals and post-parenthetical neo-literate individuals. In this construct, the pre-parenthetical insurgent and the post-parenthetical neo-literate will have more in common with each other than with the Westphalian institutions, including security organisations. On the other hand, the nation-state remains the most powerful political actor, despite long warnings of its erosion and collapse. Like individuals and other organisations, states master technology and are sometimes at the origin of its development; some are also producing new threats, sponsoring hacking and other online activity to collect information from their citizens or foreign states.

Finally, the evolution of the media changes not just what we think, but *how* we think. This change points to an insufficiently studied and poorly understood area of knowledge: the impact of digital technology on our lives. How we imagine our body, space, time and society is changing as quickly as the means with which we communicate and share information.

Our Poly-Social Selves

If we are in the midst of a societal transformation, a shift of our underlying technological organisation from the world arising of the printing press to one stemming from digital information technology, then there must be effects on individuals, too. What does it mean to be a person in a world of information networks? What does it do to our sense of self, or to our physical and metaphysical sense of place? What does the self look like after the linearity of Gutenberg's world?

It can be argued that we have reached the end of the singular perceived self and that we now exist, online and offline, as multiple identities, multiple selves, in multiple simultaneous realities. Take the example of a taxi driver whom a presenter at the conference encountered in Calcutta. As

they drove in from the airport, he pointed out a village in which he lives a parallel, virtual life. In an online iteration of that village he is married to a second woman. In this other life, he explained, he "married for love."

What does this tell us about multiple selves? Is one more real than the other? Is one virtual and cut off from the real? We may indeed be observing the end of the singular perceived self and the slow emergence of a poly-social reality. This poly-social reality encompasses not just the seamless blending of real and virtual worlds but reflects the multiple and simultaneous realities in which we live. While we have always had multiple identities, each could not enjoy its own, parallel evolution. We now can exist in multiple places at once and are becoming ubiquitous.

Therefore, poly-sociality does not just imply multiple identities, but rather splintered individuals living in separate realities simultaneously. These realities are interdependent, as something that happens in one can have consequences for another. Information distributed via social media affects all of us regardless of whether we choose to engage in it or not; and, at a societal level, what is trending on Twitter one day affects our behaviour the next.

It goes without saying that being poly-social and ubiquitous has wide-ranging repercussions. This notion adds to and complicates our Gutenberg metaphor, which is itself quite linear. When we consider the closing of the parenthesis, we do not know whether this closing spells the return of an older order or a movement forward to a new phase. It also suggests that the shift between stages could be gradual and sequential. It may in fact be more appropriate to conceive of the informational transition as a big bang. In this way the transition may be more akin to a paradigmatic jump than an orderly transition from one way of relating to information to another.

Our sense of space is challenged if we can exist in multiple realities at once. It no longer makes sense to think of "cyberspace" existing in opposition to, or in another place than, reality. Characterised by an absence of consensus, save for brief periods perhaps, cyberspace is indeed becoming part of our reality. If the 20th century witnessed significant efforts made by political power and elites to herd people into one specific identity to better provide for and control them, the 21st century will see organisations and individuals monitor, surveil and engage with our multiple selves across spaces and time.

Does a poly-social reality necessarily involve a completely different way of thinking, a rewiring in a neuroscience sense? Neuroscience posits that humans are malleable and that their nervous system can adapt. This

neuronal plasticity could influence our perception of ourselves and we could be nearing the end of the "modern self" (i.e. the self-contained, self-reflective and isolated individual). However, the speed at which we can adapt is the subject of much discussion amongst scientists; the promises of ubiquity made by technology are understandably fascinating, but the legacy of millions of years of neural development in humans must be contrasted with the few decades of network technology.

There are three ways of looking at the implications of this new self. Some believe the new self is inconsequential, that an aggregated unified self is a cultural phenomenon like many others before, and one to which we will easily adjust socially and psychologically. Others view it with concern and fear that the modern self is saturated by multiple voices, none of which are authentic. Between those extremes is the view that living a poly-social reality is becoming a way to address personal issues brought on by modernity and to become masters of self-presentation and self-creation.

The Fifth Estate

If the Gutenberg analogy helps us conceptualise the social transformation and poly-sociality defines the influence of this transformation on ourselves **as individuals, the "fifth estate" is a concept that frames the social** regroupings occurring in a world enabled by digital technology. In the 18th century, Edmund Burke argued that, in addition to the three actors in society with power and authority (clergy, nobility and the commons), the press were creating a new force of authority and should be considered the fourth estate. We can look at the emerging empowerment of networked **individuals not just as the manifestation of passing mobs, or as a** fragmenting civil society, but collectively as a fifth estate and a social actor with political influence. This estate is empowered by the nature of the information system thanks to which it exists and is organised.

As the very nature of the fifth estate threatens the other four, it presents a challenging paradox in that it could cause the entire estate order to break down. Alternately, it may be that it will not survive and that it will be co-opted by existing institutions unwilling to reform. Faced with existential disruption, those institutions may use their power to control the politics of civil society as we have seen autocrats attempt to do in Iran and Syria.

In this context, what is the fate of 20th-century institutions, or the other four estates' modern-day equivalents (intellectuals, business persons, politicians, journalists and mass media) in a world of networked and influential individuals?

Together, these three theoretical frames provide analytical clues to understand how our rapport with information is changing and what this means for public institutions. We now turn to the attributes of the new information technology world itself.

Instrumentality of Media and Information Technology

If we are in the middle of a societal transformation from a printed age to a digital age, then what are the central attributes of the networked age? Information technology has become indispensable to human activity and affects individuals' thoughts and behaviour. In particular, it is changing our notions of power, authority, cohesion and transparency.

Power

Makmende (a fictional tough-guy character) was Kenya's first viral Internet sensation. But when Kenyans tried to create a Wikipedia entry for him, it kept being deleted. Wikipedia editors, based mostly in the Western world, did not know of Makmende and removed the content because they thought the character was not significant enough or simply did not exist.

While Internet access is quickly growing, most people in the world remain without access and, for example, there are low total numbers of users and low overall penetration in the southern hemisphere. But as more people access the network, the physical digital divide becomes narrower.

Although access increases, online power does not. The Internet as a network is characterised by traditional patterns of visibility and agency. Power on the Internet is therefore not a function of access, and technological infrastructure is by no means a determinant of increased online participation. Online power instead tends to reflect pre-Internet measures of knowledge production. For example, the world's wealthiest countries have more per capita newspapers in circulation than the rest of the world; similarly, the United States and the United Kingdom produce the majority of indexed academic journals.

We can now measure new forms of Internet knowledge production and see very similar patterns. For example, if we normalised Wikipedia articles by population, language and access, Africa remains underrepresented. Power, therefore, is not explained by the uneven geographies of access. One variable that needs to be considered is mobile access. If

the developing world connects in large part using mobile devices, this access method will affect their online behaviour.

Power in the age of shifting networks must also be analysed from the point of view of nation-states. Beyond the organic evolution of the Internet and its adaptive use by individuals, governments will remain tempted to resort to new and more traditional technologies to communicate proactively their own visions of the world. The rapid emergence of new international news broadcasting services (for example, in Russia, China and Iran) signals the beginning of new forms of state-to-state conflict, as carefully crafted messaging is broadcast with political objectives in mind.

Authority

Ipaidabribe.com is an Indian Web site that allows users to upload details of bureaucrats seeking illicit payments. At the time of writing there were over 400,000 reports of bribery, covering all manner of routine government services. Reports are filed anonymously and can be neither corroborated nor refuted. The Web site is not a tool of criminal justice, but one of mass popular opinion through which Indian citizens shame the Indian government and challenge its authority.

As control over information becomes less effective, institutions have more difficulty retaining authority based simply on historical credibility. Legitimacy is now easily undermined unless hierarchical institutions can convince an increasingly sceptical public of their utility. In a new media environment, authority is earned and not assumed.

Decreased deference for existing systems and abstract authority conjure up at least three possible futures. In a first scenario, individuals may become fiercely attached to the narrative that they consider to be correct, and we may see attempts to block access to other narratives and arguments (e.g. extreme and irrational nationalism or religiosity). This is a form of media selection bias that one often finds in online ideological communities. In a second scenario, all narratives are increasingly perceived as arbitrary, leading to the complete dissolution of claims of authority and the absolute reign of relativism. We are beginning to see this in areas of the news industry. As a final scenario, we may be entering a period in which the contestation of authority has been democratised and a matter of routine. In this world, traditional legacy structures are broken down and challenged, but new institutions, with new forms of authority, will emerge. Authority is no longer conferred by the medium ("if it's in a book it must be true" or "if a government did it, it must be best") but instead shifts continuously thanks to real-time evaluations and

mass feedback, like what we see on ipaidabribe.com. The latter scenario presents important challenges to government institutions if they are to continue, in democratic governments at least, to represent the interests of the nation-state, including collective security.

Cohesion

The new information technology world is fragmented. While people continue to consume media from legacy content providers, the range of content created and consumed is expanding rapidly. This expansion is leading to a large-scale fragmentation of our discourse.

For example, a recent Pew study cited by a presenting expert during the conference analysed the ways in which US citizens receive local news. The results pointed to a complex local news ecosystem, with people relying on different platforms for different topics. There does not appear to be a horse race between old and new media, but rather a continuous blending of news sources. In addition, 41% of adults claimed also to be local news *producers* by sharing links, creating content, posting news, playing a role in the stream of local news or providing their own content. The major news divide between content producer and consumer is therefore also being bridged. Media must now be seen as fragmented not only in forms but also amongst producers and consumers. This applies to local news consumption, as well as regional and multi-language use around the world.

Transparency

As vast amounts of information are available to anyone at any time, the question of which information is public and which is protected is increasing complicated. The protected nature of information is further challenged by organisations whose very purpose is to make protected or private information public at all cost, as demonstrated to alarming effect by Wikileaks and Anonymous in the past three years. If some welcomed the improved transparency to understand for example the political stability of Iraq, many others thought that the mass publishing of US Department of State diplomatic cables was crossing a line.

The following three situations illustrate not only the continued need to control information, but also the ongoing challenges to controlling information in light of security implications. Many NGOs co-operate with governments in conflict zones; when the Wikileaks documents were released, there was a genuine fear that specific individuals would be

in danger. Also, diplomats document atrocities and sensitive political situations, which often requires that they maintain relationships with dissident sources in repressive countries. Revealing identities in this context puts lives as risk and prevents the normal conduct of diplomacy, for which confidentiality is vital. Finally, organisations, NGOs, journalists and researchers working in complex security environments often have large databases of contacts. Making those contacts public, even inadvertently, could obviously create risks and threats.

However, the challenge for governments is that part of public opinion believes all citizens should have a right to access all information collected or created by the government, while many, who point to examples of official documents that could have been overly redacted or inappropriately classified, start questioning the need for secrecy and confidentiality.

One approach to this challenge may be to make it the default position that the public should know almost everything. The only way to respond to the growing public demands for greater transparency may be to release information more proactively while continuously explaining why certain classes of information, like medical records or files of core import to the national interest, are not made public.

The Challenges Facing Democratic and Autocratic Governments

The new information technology architecture challenges all hierarchical organisations: news companies, blue-chip corporations, national governments and multinational organisations such as the United Nations. A public empowered by information formulates new demands on the state and has new expectations of the relationship between a government and its citizens. Two sets of governments are best discussed separately: democratic states face issues of privacy, public perception, authority and data policy; while autocratic states, which can manipulate technology to advance their national interests and delay democratic developments, can face existential threats from an emboldened and knowledgeable population.

How does the state deliver health care when self-diagnosis reaches full fruition? How does the government provide public education, when citizens can monitor and evaluate the quality of teaching? These are domestic-policy challenges, but the question becomes even more sensitive when considering the state's security apparatus. Areas to explore include the impacts on intelligence agencies, law enforcement organisations and the armed forces.

For Intelligence Services

The information age brings opportunities and threats to intelligence services. The central job of government intelligence is to process information and be aware of gaps in understanding; services are literally in the business of interpreting information flows. Value is derived from finding material and information of which other parties are not aware, or at least finding them sooner. Increasingly, in an age of information abundance, an intelligence organisation derives tactical and strategic advantages from better analysis, rather than greater collecting. This shift generates significant changes for intelligence, which has the unique function of producing politically relevant knowledge from publicly available information and information obtained through covert means.

In a social media world, information surrounds us. This abundance of information provides tremendous opportunity for intelligence agencies: data that is shared openly can be mined for information, analyzed for patterns, scanned for sources and tracked for investigations. This data can also be used to assess whether a piece of information is valid. Online information moves quickly and therefore so too can investigations.

This information abundance presents real challenges, however. The first is how to deal with a massive amount of real-time information. Many intelligence agencies speak of the problem of "drinking from a firehose," when referring to information management. Looking for the proverbial smoking gun is extremely difficult, so intelligence services work ever more collaboratively with allies and produce enormous amounts of intelligence, which they share increasingly. Agencies do not want the taps to be turned off, but also do not want to spill anything on the floor. This is in essence a filter problem: how to sort the relevant pieces from a big data flow.

Second, in an era of questioned authority calling for more complex analysis, it is difficult for an intelligence agency to balance its need for certainty with the realities of fluctuating, real-time data. Like all organisations, agencies could not eliminate unpredictability in the past, but the relative absence of data made it easier to achieve some degree of certainty. In light of the substantial disinformation campaigns waged online, the complexity of truly "knowing" is indeed daunting.

Third, intelligence, like the information that underlies it, is a commodity. That means that certain functions traditionally fulfilled by intelligence services can at times by delivered by other parties. Information abundance means that agencies also compete for the attention of their clients, who have greater access to alternative sources. In some cases, private organisations (Economist Intelligence Unit, *The New York Times*, the

BBC, the Brookings Institution) can provide high-quality information and analysis.

Intelligence agencies are of course more than just public data organisations and serve a unique function. They must fulfill their mandate while producing the most relevant analysis possible using both publicly available information and intelligence acquired through covert means. This requires them to develop greater agility to face what are growingly interdependent security risks on a national scale and globally, while remaining accountable public institutions in free, democratic and open societies.

For Policing

While many of the challenges and opportunities facing police forces are similar to those facing intelligence services, the core difference is that much more of the work police do occurs through direct engagement with the public. The police are a more outward-facing institution.

The twenty-four-hour social media and cable news environment, as well as the diversification of our online activity, changes the expectations that the public has of the police. The justice process has been sped up, at a time when more time is needed to analyze and contextualise huge amounts of information.

Police departments are facing new challenges at all stages of the traditional investigative process. First, the collection of background information is overwhelmed by abundance. Artificial intelligence may be able to resolve this in the future, but for now, police must combine traditional police and investigative work with experiments in leveraging online tools. Second, textbook police work, which involves evaluating and corroborating every source of information and every piece of data is of course no longer possible. Third, analyzing the provenance of information is more challenging in a social media world, where sourcing is often ambiguous. Finally, when disseminating information to the public at various stages of an investigation, police forces are increasingly incorporating social media. But how far this should extend remains an open question. How should the online space be policed? What does a virtual police station look like? Should there be one on Twitter, or in Second Life? All are questions at the frontier of 21st century policing.

For the State at War

When a democratic state is at war, the information landscape is transformed. This is not a new phenomenon. From the days of war propaganda posters through to the embedding of journalists, information and misinformation have always been used as tools of war. But due to the current presence of overwhelming state military power, wars are won more than ever on perceptions rather than outright military victory. The killing capacity of the modern state has led to a stalemate of force. What matters now is not just who is more powerful, but whose account of violence the public accepts. Put another way, in the information age, war is public relations by other means. In a world of constraints on force, war becomes a communicative act.

Three examples illustrate this point. First, despite its tremendous military strength, Israel is limited to a menu of tools that are acceptable to international public opinion. For example, when faced for a second time with the Turkish flotilla suspected of carrying weapons and supplies, Israeli special forces boarded carrying paintball guns, knowing that the public backlash against casualities would be ultimately counterproductive. They had the military force to stop the boat, but the act itself was more than a physical act; it was communicative.

Second, during the Iraq war, the story was widely circulated that a Baghdad vendor had been killed for selling tomatoes and cucumbers together, a supposed affront because male and female symbols were present in the same bin. This was widely believed to be true, and fuelled a backlash against religious extremism that is thought to be partly responsible for the Sunni awakening. It turned out to be misinformation.

Finally, the all too familiar example of a NATO airstrike on a convoy in Afghanistan demonstrates this dynamic vividly. Moments after a strike, the Taliban will often release false claims about the significant "civilian" casualities incurred. But it takes NATO hours, or days to counter the disinformation. In this sense, NATO is losing the information war. This example could be extrapolated much more broadly to cover the wide range of challenges of fighting a counterinsurgency war.

Opportunities for Democratic Empowerment

Whereas the challenges posed by information technology in democratic states are largely managerial in nature, the opportunities offered by information technology for promoting democracy in autocratic states are revolutionary. An autocracy is the absolute manifestation of the power of

controlling information. The fact that this control is increasingly untenable has opened a new frontier for activism, political protest and revolution.

Social media in particular has proven powerful at breaking the autocratic grip on the control of information. Autocracies used to be able to create a collective action problem, whereby the costs of action were incredibly high (death, torture, imprisonment). Public opposition for citizens was all or nothing, revolution or acquiescence, and the risk was absolute. Social media breaks this collective action problem by creating a back channel for political participation with a far lower risk threshold. The "cute cat" theory of social media proposed by Ethan Zuckerman, for example, argues that platforms like Facebook serve as Trojan horses for political disobedience. Once the sharing of cat photos is normalised, then there is the potential to share a much wider range of political information. Several examples demonstrate the ways in which information technology and social media are being used to challenge autocrats.

In Syria, the brutal crackdowns of the Assad regime are being live-streamed. However, there are real questions as to whether this documentation is in any way moderating his behaviour. The opposite is potentially the case. Since his crimes are being documented in detail, Assad has no option but total victory. Internationally, will the videos of Assad's violent regime repression just become background noise, similar to starving children?

Technology was leveraged by all sides in a wide range of ways during the protests against Egyptian President Mubarak. While Mubarak shut down the Internet and attacked protesters in Tahrir square with thugs on camels, a small group of 20-year-olds based around the world coordinated, supplied and staffed 10 field hospitals to aid the protesters, all online.

Rami Jarrar, a Syrian blogger, came within an inch of not escaping from Syria. After leaving Syria, he was travelling through Doha and was stopped by a customs officer who threatened to deport him back to Syria due to a passport problem. He reached out on Twitter for help, and someone who saw his tweet called a sheikh in Qatar who came to his rescue at the airport. A 21st-century problem that needed a 17th-century solution: a sheikh.

There are of course many cautions. We are seeing a technological arms race between autocratic states using technology to monitor, seek out, and crack down on protest (often using technology developed in democratic countries), and protesters seeking to use information technology to shame, document the atrocities of, and undermine the authority of the governments oppressing them. We are at the early stages of this new

escalation and should therefore guard against envisioning a future that is linear or drawing precipitous conclusions: new technologies will not automatically make all governments democratic. Autocratic regimes, too, are adopting technology and have the freedom of action to collect information on and control their population.

Operating in this New Ecosystem

Legacy hierarchical organisations are at a crossroads. Information technology and networked organisations both challenge and disrupt their very existence. If the organisation is a private corporation, such as a newspaper or an auto manufacturer, then creative destruction may very well be a net positive. The online news sources and aggregators *The Huffington Post* and *ProPublica*, could conceivably replace *The New York Times*, and electric car-maker Tesla Motors might replace Ford. Creative destruction is more difficult, however, in the public sector. The foreign ministries, police forces and intelligence agencies are not simply going to disappear and be replaced by start-ups. The new information environment, however, may require them to adopt some of the start-ups' characteristics.

This is of course a sweeping task. But below are several areas in which the public sector organisations can start to step out of their comfort zone and begin to rethink the social contracts and operating procedures that are limiting their transition into the digital age.

Reverse Organisational Engineering

The typical response of legacy institutions to the digital information revolution, and to the post-parenthesis world, is to shift online. For 15 years, newspapers simply moved their content to a Web site, seeing it as one more distribution mechanism. Only when facing existential disruption did they rethink what it means to do news online. Some are now starting to get it right, to innovate. For many it was too late.

The challenge for government is how to rebuild, reform, reimagine and disrupt their own institutions in order to remain relevant and to function in a digital era. One innovative idea is instead of simply moving our old institutions online, to do the opposite and look to online forms of communication and action and see if we can scale them up or use them as models for new institutions.

If the goal of 20th century was to serve one common version of the self, we must now learn to build new institutions that represent our poly-social realities. For example, what could an institution that caters to our multiple realities look like? We need to build new institutions that accommodate new forms of behaviour and rise out of new conventions. What are the new institutions evolving out of cyberspace, and how can we learn from them?

Take for example institutions of multiculturalism, which are designed to build cohesion across groups. How might they evolve in light of the public's multiple, overlapping and simultaneous identities? How, for example, could government foster the emergence of shared values?

Protecting the System

If information technology is instrumental to how organisations and government institutions function, then protecting the underlying sociological and legal system as well as physical infrastructure is a useful place for government action. This need for protection becomes even more important when, instead of a dualism between unregulated cyberspace and the real world, we see both as having the same mix of social, political and economic realities.

The first place this protection mandate is playing out is in domestic law and regulation. For example, allowing more competition in the Canadian wireless industry could drive down mobile phone and Internet rates for Canadians, who currently pay some of the highest rates in the world. Such a drop in rates would give more people access to a service that many argue is becoming essential for modern life. In the United States the widespread backlash over the *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PIPA) and *Stop Online Piracy Act* (SOPA) demonstrated that the public is becoming increasingly aware of attempts to interfere with the freedom of the Internet.

Second, much of the new digital geography of the Internet is being built by the private sector. They are the ones innovating and disrupting the communications world, which was once a strongly government-controlled industry. They are experimenting with new financial, open sourced and crowd-sourced models, such as Firefox, and building institutions that exist across traditional intuitional classifications. There is a need for government to better understand these developments and to properly incentivise similar behaviour.

Finally, internationally, governments can do much to protect the freedoms of peoples to engage online. The US Department of State

is working to protect Internet freedom precisely because they want to democratise voices to break down authoritarian power. There is also a more controversial aspect to this, however. For example, how should the US act to stop US corporations from selling technology to oppressive dictatorships that use it for the surveillance or targeting of their citizens? What if this use undermines other aspects of US foreign policy? Related to this concern, there is a debate as to whether the United Nations should be the international body that oversees the governing of the Internet. While it is in many ways the most legitimate international organisation, it is composed of nation states and is designed to protect state interest. This purpose is in contrast to the Internet, which is a transnational network of information and individuals. Can we expect states to fully protect a system that facilitates and enables challenges to their authority, especially when some of them do not abide by international law?

Embracing Big Data

The scale of data now being produced is incomprehensible to the human mind. Metaphors are no longer even sufficient. For example, we produce a Library of Congress worth of data every five minutes and five hexabytes of data are created each day.

"Big Data" is generally defined as data sets that exceed the capacity of the typical computer to manage. And this is quickly becoming the norm. This trend is leading to a new law of production, where the more we consume, produce and use data, the cheaper it becomes. Or, put another way, data is not subject to resource constraints. If "big data" is a new mode of production, then protecting cyber security should increasingly be considered a public good.

There are of course wide ranges of uses for this data. Citizens used it to mobilise assistance after the Japan and Haiti earthquakes. It allows for better corporate decision making and analysis. Some argue that US retailers can potentially increase their margins by 60%, others that the "second" online economy will reach the same size as the physical economy in two decades.

For the intelligence community, however, "big data" is both a blessing and a curse. It can be used for situational awareness, to predict the size of a demonstration, to understand what groups think about specific issues, to detect spontaneous events, or for the surveillance of individuals. This upside is mitigated, however, by the physical challenges of dealing with such massive data flows. There are also analytic challenges. The government's use of big data requires that more resources be devoted

to social sciences. Algorithms have limited utility if they are not designed properly or if the meaning of the data is misinterpreted.

There are also real ethical challenges. How should government use the big data that they collect? There are a number of principles that could be followed. Government should have sufficient cause and integrity of motive. Use of data should be proportionate, necessary and under the right authority, validated by external oversight. Data investigations should have a reasonable prospect for success. Finally, the litmus test for the use of data should be whether the government would be willing to stand in front of the public and justify its decision.

Rethinking Education

Finally, in the new information technology world, literacy has taken on a whole new meaning. It is no longer enough to train our citizens to read, write and do basic math. They need to become aware digital citizens, regarding both the content they are consuming and the technology that underlies it. This means that they must have much better critical thinking skills to judge credibility, accuracy and authority. To achieve this goal, awareness of logical fallacies should be taught at the heart of education. The public must also understand the physical and software infrastructure on which the digital information world is built. This means knowing how algorithms deliver them the news, how open-sourced editing works, and how the demographics and biases of computer programmers affect the world they engage in. The pitfalls of disinformation and dynamic of a networked world require that basic computer programming and the ability to protect one's privacy be taught widely in future.

Conclusion

Information technology and the vast changes to the media world it is facilitating are transforming the way the world works. Turmoil and transition in the media industry is both a literal demonstration of shifts in information technology and reflective of the challenges facing all legacy institutions. Any institution that in the 20th century relied on, and gained power and authority through, the creation and control of information, is being challenged by a new global information ecosystem that erodes the foundations of hierarchical systems.

In this way, intelligence agencies are very similar to news organisations. Their value lies in their ability to know about and analyze events quickly

and accurately. But government institutions face a unique challenge. Whereas disruption and creative destruction are forces that can have a positive and innovative collective impact on a business sector (such as media) this net positive requires a possibility that legacy institutions will be replaced. In the media world, this means Internet start-ups competing directly for readers with *The New York Times*. While *The New York Times* is an excellent newspaper, it is not inconceivable that an online competitor, freed of legacy costs such as printing presses, delivery trucks and labour unions, could replace it.

Government intelligence organisations, however, cannot be replaced by start-ups. This means that disruptive change will have to come from within and that the organisations themselves may face periods of self-reform. They must determine in what areas they add value and shed others in which they do not. They stand to gain from the innovation occurring in the realms of information, technology and data, even if these innovations imply difficult choices such as adapting to evolving mandates and rethinking their relationship with the public.

2
Panel Summaries

Panel Summaries

The Evolving Definition of Expertise

The End of the Gutenberg Era

The first speaker addressed the changing dynamics of the current information revolution in an historical context. Drawing parallels from the changes in society brought about by the invention of the printing press, the speaker argued that new emerging technologies were revolutionising society. The Gutenberg era is marked by the notion of a single, complete linear narrative. All knowledge and information is presented in a contained form: words are written in margins, which are contained in books, which are stored in bookcases. Knowledge is therefore static and presented in a contained form.

While the invention of the printing press sparked a Gutenberg era of "containment", new emerging technologies are introducing a new era of what the speaker termed "connectivity". In this new era, information is dynamic and connective; information is shared across a variety of platforms and is open-ended. In this new era information becomes shared among a larger number of actors, and changes with each individual performance. This era of connectivity, argued the speaker, shares similarities with the pre-Gutenberg era, where information was transmitted orally between individuals within communities. The narratives passed on in these communities were open-ended and changed with each individual's interpretation of the story. As a result of the similarities between these two eras the Gutenberg era is a brief interruption, or parenthesis, in the course of human history where information is connective.

The significance of these various eras of information sharing, the speaker argued, have significant implications for society and the way individuals think. In the Gutenberg era there was a close relationship between the way information was presented to a community and the latter's way of life. The journalist was the gatekeeper of information and the contents of journalism influenced people's beliefs and allowed them to approach reality in terms of categorisation. As this era closes and information becomes once again uncontrollable, categories will erode and a potential "rewiring" of humans' cognitive abilities may take place.

The speaker pointed out a few potential implications for society and security of this hypothetical rewiring. Individuals from the pre-Gutenberg era, for example the tribesman in nomadic regions of the Middle East, might have more in common with the emerging post-Gutenberg

individual than a person from the era when information and knowledge were contained. Conflict will come from those who think in terms of categorisation confronting a new era of pre- and post-Gutenberg individuals who think in terms that defy categorisation. Problems that may present themselves as social, religious, or ethnic in nature can be translated into mediums of communication and the way individuals understand their world. Concluding, the speaker reiterated that as post-Gutenberg actors are empowered through emerging technologies, there will inevitably be conflict as society changes and adapts.

The Internet is Like Water

The next speaker also discussed the implications of the changing dynamics of information. Beginning from a description of the previous century, the speaker demonstrated how technology allowed information to be structured in a way that favoured the elites. The means of communication such as newspapers, radio, and television were expensive to own and had the capacity for a small group of individuals to send information to large masses of people. The result of this was high barriers to entry that allowed the elite to control the means of information and dictate what information was important and what the public should focus on.

As a result of both the Internet and revolutions in technology, the structure of information sharing has dramatically changed. The speaker used the example of an $80 mobile phone that provides the technology of a radio station, a TV station, and a newspaper in one hand-held device. The result is that the Internet and revolutions in technology have thus lowered the barriers to entry for information-sharing and has compromised the power of elites to control information.

Examining the consequences of these changes on society, the speaker argued they have caused people's attention span to shrink. People have the ability to choose what information they want to pay attention to, and that differs increasingly from the elites' expectations. Thus, the speaker argued, legitimacy is less and less deserved as a result of technology, and individuals, institutions and media must redouble their efforts to draw the attention of the masses. This, in turn, leads to a much more profound implication for society.

With the elites no longer able to determine what people consume intellectually, they have much less power to dictate narratives of truth and identity. The competing narratives now available as a result of technology, according to the speaker, could potentially result in two

different futures: one may be that people may cling fiercely to the narrative that they consider to be correct and attempt to block access to other "truths" or arguments; the other potential future is that all narratives may be viewed as arbitrary in the minds of citizens. The internet therefore has a serious capacity to destroy belief systems and tear institutions apart. The most serious implication of this information revolution is that "it [the Internet] is more adapted for people to say *no* rather than *yes*", in other words it makes it easier to break things down and to challenge existing realities rather than build new ones.

Discussion

During the panel discussion, one individual argued that, despite some potentially negative effects of the information revolution, it also provides benefits like the ability for people to contest authoritarian regimes. The speaker highlighted the fact that one of the long-term repercussions of the closing of the Gutenberg era is that authority is no longer conferred by the medium ("if it is in a book, it must be right"). If it makes it ever harder—and perhaps impossible—for shared narratives to emerge, how might the notion of collective (national or other) security or even social progress evolve?

Gauging the New Information Era

The Internet as the Fifth Estate

Using the historical analogy of the estates of the realm, the first speaker in this series argued that the Internet is becoming a new actor in society that is able to garner trust and respect from citizens. In pre-revolutionary France, three estates constituted authority: the clergy, the nobility and the commons. The 18th-century political thinker, Edmund Burke, argued that the introduction of a free and independent press established a fourth estate. The speaker argued that each estate has a modern-day equivalent: intellectuals, business elites, government and journalists. If in the previous century authority was made up of those four estates, the speaker argued that technology has allowed the Internet to become its own source of authority in society, creating a "fifth estate". The speaker based this argument on the fact that individuals increasingly rely on the Internet to learn about the world as much, if not more, than on television broadcasts and newspapers.

One of the major implications of this new estate is that it has allowed the protestor to become a more relevant actor in society. Using examples such as the recent opposition to proposed changes to Canada's Privacy Act, the speaker highlighted the ways in which the fifth estate is able to generate support from a critical mass of individuals to raise issues and affect government policy. He expressed scepticism, however, as to the fifth estate's ability to survive as it faces challenges from all the other actors in society that do not wish to see their authority challenged. The Internet's fluidity and freedom should not be taken for granted. One may also ponder the implications of the lower "cost" of protesting on a country's political life. If it is ever easier to oppose specific measures, projects and proposals, shallow protest action risks generating a shallow response, nurturing an "easy-fix generation".

How People Learn About Their Local Community

The next speaker presented survey findings on how local communities in the United States consume information about their immediate environment. The survey was conducted on 16 different local news topics and analyzed the individuals' changing habits. The findings presented a complex picture where individuals rely on multiple platforms to gather information on different topics.

Although the results of the survey indicated that there is no clear winning technology or media platform for news, important trends emerged. For adults under the age of forty, the Internet was the most used source for 11 of the 16 topics surveyed, indicating potential generational preference. Also, the majority of individuals thought that their local newspaper was important even if 67% of them thought that there would be no impact if its publication ceased; the newspaper may be important but is not valued. Finally, mobile phone apps have very little "sticking power', with people demonstrating no loyalty to media apps, which are deleted as quickly as they are downloaded.

Geographies of the Internet

The third speaker in this series presented findings about online participation in emerging economies, referred to as the Global South. One of the potential benefits of the Internet and improved access to information is that it can create conditions to empower historically marginalised groups. For this to take place, however, several barriers need to be eliminated. One is addressing the relatively lower numbers

of Internet users in the Global South and narrowing what has come to be known as the digital divide between affluent and less advanced economies.

The speaker addressed whether individuals in the Global South, once connected, are using the Internet to project political power. In order to gauge the level of participation, he presented studies of the number of Wikipedia contributions coming from individuals from historically marginalised regions. The study found that there is a significant lack of representation from individuals in the Global South and that this lack of representation cannot be explained by unequal Internet access alone. If we remove this variable, the study demonstrates that lack of political participation continues to reflect traditional patterns of underrepresentation.

Discussion

During the discussion period, a participant stressed that to access the Internet most people in the developing world use hand-held devices, which may not yet be suited to editing Wikipedia entries. In the United States, non-white individuals rely much more heavily on mobile devices for access to the Internet than white persons. While the technology platform is important in itself, a participant said there are many questions left unanswered about representation: who represents whom on the Internet, and might security problems arise from this?

Big Data

Big Data: a Double-Edged Byte

The first speaker in this module discussed "big data" from an economic standpoint and argued that it can be seen as both an enabler and disrupter for growth. Describing what is meant by big data, she said it refers to data sets that exceed the typical size of data sets that are considered easy to manage. Amongst the trends she saw deriving from this concept is the democratisation of data, where information was once only available to a few people is now becoming available to most. Addressing the sheer enormity of data being created, the speaker indicated that five exabytes (1,000,000,000,000,000,000 bytes) of data is being created a day globally.

The speaker then began to discuss the implications of big data, the first of which is the phenomenon makes mobilisation much easier. She cited the response to the Japanese earthquake in 2011 and the Occupy Wall Street movement as ways data and its availability can rally people. The second implication of big data is its productive value as a new economic factor of production. The speaker said that data has led to better decision-making and analysis, generating $600 billion worth of consumer surplus worldwide. The third implication is that big data is creating a second economy that, it is estimated, will reach the size of the physical economy within two decades. Concluding her presentation, she underscored the potential for big data on society can be both positive and negative, enabling and disrupting growth at once.

Big Data: Many Sources, One Environment

The next speaker presented two cases to illustrate how big data has affected society. The first dealt with an Iranian rocket launch. The photograph of the launch had been tampered, presenting what had been a failed launch as a successful one. Many mainstream news media in the Western world failed to spot the fraud and reported on the launch as if it had been a full success. Many online observers, however, had already exposed the fraud hours before any reports were made. The failure of the press to use a wider range of sources and detect the doctored photograph, according to the speaker, illustrates a failure of using big data.

The second case described efforts by friends to locate a lost sailor using satellite imagery, computer imaging and programs like Amazon's Mechanical Turk (a marketplace that makes it possible to compensate individuals given small tasks). The speaker argued that this story highlights the many disciplines needed to take advantage of big data. Both instances provide a case from which security services can learn.

Social Media Analytics and Intelligence

The next speaker presented on the need to incorporate social media analytics into security and intelligence practices. He recounted a study conducted on the English Defence League, a political group that demonstrates publicly against Muslims in the UK. Using social media, data was obtained on the League's members and sympathisers and cross-referenced with where they lived to find out how many people could show up at a particular demonstration. Using this information,

he argued, the police were able to better deploy resources. Using this story as a backdrop for the rest of the presentation, the speaker argued that social media needs to be used creatively by security services. Citing the example of the 2011 riots in England, he contended that if the police had paid closer attention to social media, they would have noticed an alarming spike in activity preceding the events.

The speaker also stressed the need to respect privacy and outlined six principles that should be considered when deciding to undertake social network analysis: 1) there must be sustainable cause that provides clarity on why, when, and how social media analytics is used on a population; 2) there must be genuine grounds for gathering intelligence; 3) information gathering must be proportionate and necessary; 4) use of social networks analysis must be sanctioned by authority and validated by external oversight; 5) there must be a reasonable prospect for the data to turn into something usable and valuable; and 6) the recourse to secret intelligence must be a last resort.

Discussion

During the discussion a question was raised as to how to deal with disinformation and whether there is value in trying to correct falsehoods. One of the panellists said it is important to have individuals in place to respond to developments in social media, counter rumours and identify trusted sources to disseminate information further. Another panellist provided an example of how governments have used social media to improve government programs: one government published a mortgage application form online and invited individuals to comment on its design. Both panellists stressed the need for governments to become more aware of social media trends and to consider more ways to engage the population through such networking.

Social Media in the Political World: New Player, Old Game

The speaker underscored the importance for governments of recruiting social scientists to help make sense of big data. Data without insight can be very misleading and analysts with a background in social sciences are crucial to understanding these new developments. She also argued that it is important to differentiate the way in which social media work in advanced democracies from autocratic societies like those in the

Middle East. Using the Arab revolts as the backdrop to her argument, she stated that social media is increasingly being used as a means to solve the collective-action problem of challenging authoritarian regimes. By acting as a means of co-ordination, social media enable a back channel to come together and address the collective action problem of resistance to autocratic regimes.

Illustrating her thoughts, the speaker contrasted the uprising that took place in Tunisia in 2009 and which gained no traction; in 2011, however, social media played a role in galvanising the population against the government, the country then counting two million Facebook users. These changes have profound implications for politics and civil society which we are only beginning to understand.

Dilemmas and Vulnerabilities: What Shifting Information Means for Governments and Intelligence

Challenges to Security in an Information Age

The speaker presented some of the challenges for intelligence organisations in the new information age. One of them relates to the image of intelligence services, which have increasingly to defend their existence and counter negative stereotypes too easily associated with them. Another challenge is to develop products that are unique and valuable to governments and their public. In an era where data is widely available and cheap, the speaker spoke of the constant effort to remain relevant and provide useful information to their clients.

He also addressed the advantages and disadvantages of relying on social media. The latter provide a wealth of constantly updated information that can be mined and exploited; it also makes it possible for individuals to network broadly. There are disadvantages, however, including the so called "drinking-from-a-fire-hose" effect, which describes the challenges that intelligence agencies face in managing massive volumes of data and filtering information without losing important elements.

Policing in the Information Age

The speaker outlined the changing context of information, stating that it poses both challenges and opportunities with regards to law enforcement.

One challenge is the collection of information: the overwhelming volume of information has made it difficult to gather relevant and useful information. The speaker expressed hope that at some point in the future artificial intelligence would facilitate information collection; collection would come from a merger between traditional policing and online work. Another challenge for policing is accountability and transparency; when gathering information, it becomes necessary to document when you became aware of the information and be accountable for how it was gathered. Other challenges pertain to analysis (ascertaining whether a source is independent) and dissemination (how to spread policing messages). The speaker also outlined future opportunities for policing, such as creating virtual police stations or other mechanisms to allow for safe experiences on the Internet.

Who Needs Secrets

Another speaker stated that "the public has a right to know almost everything", but recognised that some information must be protected by the state. In the world of non-governmental organisations (NGOs), it is generally believed that all information should be released, many considering it almost treasonous to add any nuance to this position. There is logic to this reasoning because NGOs need information to do their work, but there remain limits to what should be made public. Using four examples of situations where information should not have been released, the speaker demonstrated that in many cases individuals can be harmed by information released (as in the case of Wikileaks) or that it can hurt the reputation of some NGOs (if they are seen as co-operating with certain governments even if it may be reasonable to do so). The speaker concluded by asking individuals to treat NGOs with understanding, as well as to recognise the unique position they occupy in society and the responsibilities that entails.

Discussion

A participant asked whether Wikileaks made source recruitment more challenging. The panellist responded that some sources recognise that there is risk, but many believe that the information they provide will make a meaningful contribution to countering threats. A speaker commented that it is inefficient and inappropriate to have intelligence operations led by Internet service providers alone and stressed the need for a regulated, transparent approach.

Of Contents and Vessels: The Slow Divorce of News and Traditional News Outlets

A Look at the Newspaper Industry in the United States

According to the first speaker the survival of the newspaper is important for the continued strength of democracy. He said that the most important part of a newspaper is "the iron core", that 15% of information that provides verification in the areas of politics, business and civil society.

In the US, unlike many other countries, the industry relies heavily on advertising as a source of revenue. The 2008-09 recession led to large operating losses and difficult financial times. The problems, however, may also have saved the industry. The enormous profits made in earlier decades allowed newspapers to take on long-term, financial commitments (pensions, pay-outs), making them more complacent and less able to innovate. The shock of the recession has forced the industry to re-think its business model and focus on local markets to which they are uniquely positioned to deliver news. He concluded on a hopeful note, arguing that newspapers can survive in this era if they concentrate on delivering local news with a strong emphasis on the "iron core".

How Do Newspapers Fare Globally?

The next speaker recognised that newspapers may be businesses but that they serve a unique function in society and that fears of the demise of newspapers are exaggerated. Newspapers still have the biggest reporting teams in media journalism, despite recent cuts, and outside North America, where the focus is debt repayment, the industry is investing in digital technologies and gradually moving towards structures where digital activity accounts for half of all revenues.

Elsewhere in the world, revenues are derived in almost equal parts from circulation and advertising; individuals there are willing to pay more for their news, making newspapers in Europe and Asia more resilient. The speaker highlighted two final points: circulation of newspapers is still growing worldwide, and the continued capability of merging digital and print media will be an important factor in the industry's success in the future.

Balancing Coverage and Business Realities

The third speaker outlined some of the changing dynamics of the newspaper industry and how its adaptability will allow the industry to survive. A new trend is the growth of social media in the realm of journalism. Newspapers have not fully exploited this new technology and look uncomfortable in using it.

One of the effects of social media is a greater diversity of stories to cover with, however, fewer resources devoted to each. Another is that stories now have more depth. Previously a newspaper acted as an omnibus publication and considered an issue was "covered" with limited information. The use of the Internet now allows for stories to be explored at a much deeper level and presents an enormous amount of potential coverage.

The industry will face a key challenge in North America that can hamper change: legacy costs (pensions and benefits) from the previous era form a significant obstacle to investments in emerging technologies and platforms.

Discussion

A question was raised regarding the sustainability of newspapers resorting to "pay walls" for online contents because so much content is already available for free elsewhere on the Web. The panel's reaction was mixed. One speaker argued that very few newspapers will successfully use a pay wall (for example, *The New York Times*), and that many of the lesser known papers will simply fail if they do so. The other panellist indicated that creating methods to pay for online content is the only sustainable way for newspapers to succeed in the future, and that implementing a model that would allow for this is imperative.

How Media Are Influencing What People and Society Become

Focussing on the societal consequences of trends emerging in civil society as a result of social media, the presenter began by recounting two anecdotes describing how individuals are increasingly using social media and the online community to project identities that individuals are prevented from exhibiting in the physical world. In introducing her thoughts on social media, the speaker returned to the Gutenberg

parenthesis arguing that it was too linear an analogy; social changes brought about by media today are better understood as a "big bang", or total disruption from the past. Drawing from neuroscience, she said that human thinking is adapting fast to the new reality because it is infinitely malleable. As a result of our plasticity, we are experiencing an augmentation in the way we think and interact. Contrasting emerging trends with the former modern self, the speaker argued that, whereas the self previously was contained and was limited to certain identities that we projected sequentially to others, new technologies allow us to project multiple identities at once. We are entering an era of poly-social reality, where the online and physical worlds blend seamlessly. The implication of this is that we are becoming ubiquitous; we can live in several augmented identities within different realities. Concluding her presentation, the speaker stressed that it is important to approach these changes with caution; we must certainly allow the self to expand, but not lose sight of our values.

Discussion

One salient point raised during the discussion was that, while the physical and virtual worlds may at times seem to merge, cyberspace does exist separately. The physical infrastructure that makes cyberspace possible is controlled by private corporations and has significant implications for privacy and surveillance. In response, a panellist argued that it is important to abandon the real-v.-cyber dichotomy because cyberspace implies that the virtual world is unregulated. This touches on an important paradox: whereas the 20th century was about "herding the selves into one constructed identity" (creating nations, classes, etc.), technology allows once again for multiple identities, but could unprecedented surveillance power and monitoring potentially act as a means to herd the selves again?

Is There a Race Between Big Powers for Global Attention?

Is war politics by other means? The speaker contended that this axiom is no longer true and that instead "war is *public relations* by other means". He said that the killing capacity of humankind has grown so great that it has almost lost its relevance. As a result, the objectives of conflict are controlling international public opinion and garnering support for one's cause, society or country. Illustrating this point, the speaker discussed Israel's military capacity to obliterate Iran and that, while it may be in

its interest to do so, it cannot because of international public opinion constraints on what is deemed to be proper international behaviour. Increasingly, the success of a war will reside in having convinced the international community that legitimate means are employed for a legitimate cause.

Consequently, the West must do all it can to counter disinformation. For example, whenever a drone strike is conducted in Afghanistan or Pakistan, the Taliban instantly claims that the victims were all innocent civilians. The Taliban can quickly circulate false rumours but it takes days for the United States or its allies to verify and counter such claims. Concluding his presentation, the speaker reiterated that it was imperative for free and democratic states to do all that is possible within their means to correct potentially damaging statements of disinformation.

Discussion

A participant commented on the media's role in correcting disinformation and presenting truth. The speaker responded by stressing that the media needs to be more critical in what they present as "truth". The speaker warned of "communities of disinformation", ie. interest groups provide false information, and that the media needs to be more sceptical of these communities as reporting on biased findings could have significant political consequences for other groups in society.

The Geopolitics of News Media

Soft War and Strategic Narratives

The first speaker discussed how media is used to achieve political objectives and the implications this has for international ethics and norms. He explored the differences between soft power and soft war in the context of "a quiet arms race", with certain countries acquiring the capacity to reach into the media of another country. Soft war, the speaker argued, is the strategic and focussed use of non-military means to achieve objectives such as regime change that might otherwise be obtained through conventional power.

Successful soft war leads a system of government to disintegrate from within. By using media to challenge other people's beliefs and undermine domestic values in a given society, countries can destabilise

governments and achieve their political ends. The message presented must be effective at undermining internal values. Iran, for example, already has a cabinet-based strategy to respond to soft war attacks.

Al-Jazeera: Bridging and Dividing

The next speaker provided an analysis of the role of the Qatar-based broadcasting station Al-Jazeera. Beginning with a brief history of the station's development, the speaker argued that Al-Jazeera had allowed the populations of the Middle East to see themselves from their own perspective rather than through the eyes of the West. Qatar created the network to promote its role as a leading power in the Arab world. The network has made it possible for many unconventional and taboo issues to be addressed. Its impact has been enormous and has helped change the social and political dynamic in most Arab states.

The West's reaction to Al-Jazeera was initially one of distrust, which was altered somewhat by the indispensable coverage it provoked in the early months of the Arab revolts. The presenter suggested that in light of Al-Jazeera's reach in the Middle East and elsewhere, Western governments may wish to increase their visibility on the network. By increasing the availability of Western leaders for interviews to explain policies and foster dialogue, the West can better address the implications of this emerging non-Western media force. The speaker also noted that Al-Jazeera is now facing competition in the region from independent local channels. From a security point of view, he also warned that its discourse should be carefully monitored.

China's Broadcasting Ambitions

The next speaker stated that the rise of Al-Jazeera garnered a lot of interest in China and influenced the country's broadcasting ambitions. Mao Zhedong's vision of the media as a megaphone for the Communist Party has not changed since 1942 and continues to play this role in China today. It is also a tool for the collection of intelligence for the Chinese authorities abroad.

China has become fixated on the idea of soft power to match its economic and military strength. This policy has been met with mixed success, as planners have failed to appreciate that credibility cannot be manufactured and has to grow organically. The Chinese are attempting to make up for their shortfalls with considerable investments. At a time

when many Western media platforms are closing foreign bureaux and scaling back operations, Beijing is expanding its media presence globally. It has heavily invested in projecting its new image abroad, including through international broadcasting.

The Politics of News and Access in an Always-On Age

The Appeal of Conspiracies and Disinformation

The first speaker discussed the growth of conspiracy theories in the online world. The typical conspiracy theory contains two parts: it creates an "in-group" and an "out-group" and it positions the individual in a perpetual existential battle against the in-group. The risk, the speaker argued, is that "if one believes that one's people is being oppressed by an ignored threat, it might lead one to believe that a shock, a spectacle is needed to shake people from their stupor" and see the "truth". These explain certain mass acts of violence (eg. Timothy McVeigh's anti-government views and terrorism).

An important fact is that minority communities are the most susceptible to conspiracy theories. This has far-reaching consequences because governments often need to work with such communities and face enormous distrust. He stressed that it is critical to teach young people critical thinking to allow future citizens to detect fallacies more easily. Furthermore, all education should create awareness about technology to help children understand how open-source editing work and assess the strengths and weaknesses of sources.

Digital literacy, however, can only go so far in addressing conspiracy theories. Emotional appeal and structural inequality will always be strong factors in allowing conspiracy theories to thrive. Although these factors are difficult to counteract it is important to address the disinformation via platforms that the conspiracy theories themselves use (for example, YouTube) and expose the logical fallacies inside of them.

Media and Internet Regulation

The next speaker discussed some of the implications of Internet regulation for national governments, companies and individuals. The media ecosystem is changing the way we view politics and democracy.

In the United States, media concentration is harming democracy and the news "iron core" has decreased in importance as the valuation of objective fact has decreased.

The evolution of the media landscape once again makes local communities relevant for governance, giving way to what the presenter termed as "the rise of open source politics". In a world where the digital geography of the Internet is private and corporate the private sector has attempted to monopolise the digital infrastructure. The future will be about trying to democratise it, a peer-to-peer mobile phone service being one way in which the infrastructure of technology can become more democratic.

Security Competition and Search Skills

The moderator offered the following conclusions. To succeed in this new age of big data, institutions need increasingly to automate tasks, which also makes human beings more redundant. Given the importance of the Internet and the information revolution, the success or failure of the next generation in interacting in this new information space will be dependent on its ability to read critically and be digitally literate. We are closing a "golden age of information" and moving into an era in which individuals must be more diligent in finding information; it will become increasingly difficult to find specific information as more and more becomes available. In order to realise the true benefits of the information revolution, we must burst the "filter bubble", that is the tendency users of the Internet naturally have to seek ideas that reinforce their existing beliefs, which prevents genuine learning.

Annex A

Conference agenda

Informing (In)Stability
The Security Implications of a Shifting News and Media Environment

21-22 February 2012

A conference of the Canadian Security Intelligence Service held in partnership with Policy Horizons Canada
CSIS National Headquarters, Ottawa

Tuesday, 21 February

8.45 – 9.00	**Structure and Objectives of the Conference**
9.00 – 9.15	**Opening Remarks**
9.15 – 10.15	**Module 1—*The Evolving Definition of Expertise***
	Closing Gutenberg's era and the beginning of information wilderness *Like water: gauging the Internet's effects on organisations and society*
10.15 – 10.30	Break
10.30 – 12.00	**Module 2—*Gauging the New Information Era***
	The rise of the fifth estate: impartiality, public good, national identity and democracy *How people learn about their local community* *Mapping and measuring local knowledge production and representation: Geographies of the Internet*
12.00 – 13.00	Lunch
13.00 – 14.15	**Module 3—*Big Data***
	Big Data – A Double-edged Byte *Many sources, one environment* *Using big data in security and intelligence work*
14.15 – 15.15	**Keynote—*How Social Media Work in the Political***

	World Today
15.15 – 15.30	Break
15.30 – 17.00	**Module 4—*Dilemmas and Vulnerabilities: What ever Shifting Information Means for Governments and Intelligence*** *Practical challenges to providing security in the information age – an intelligence perspective* *Practical challenges to providing security in the information age – a policing perspective* *Who needs secrets? Exploring the open-v-closed spectrum*
17.00	Adjourn

Wednesday, 22 February

9.00 – 9.15	**Review of Day One**
9.15 – 10.45	**Module 5—*Of Contents and Vessels: The Slow Divorce of News and Traditional News Outlets*** *Justified Panic? A look at the newspapers industry in the United States* *The Flip Side of the Coin: How do newspapers fare globally?* *Understanding the World (On a Shoe String): Balancing coverage and business realities*
10.45 – 11.00	Break
11.00 – 12.00	**Keynote—*Many Sources, Many Faces: How Media are Influencing What People and Society Become***
12.00 – 13.00	Lunch
13.00 – 13.45	**Keynote—*Is There a Race Between Big Powers for Global Attention?***

13.45 – 15.00	**Module 6—*Worth a Thousand Words: The Geopolitics of News Media***
	Soft war, strategic narratives, and the reshaping of international broadcasting *Al-Jazeera: Bridging and Dividing* *Signals from Beijing: China's broadcasting ambitions*
15.00 – 15.15	Break
15.15 – 16.45	**Module 7—*Network Power: The Politics of News and Access in an Always-On Age***
	True or false: the appeal of conspiracies and disinformation *Media and internet regulation in flux across the globe: What it means for national governments, companies, and individuals* *Security, Competition and Your Search Skills*
16.45 – 17.00	**Summary**
17.00 – 17.15	**Concluding Remarks**
17.15	Adjourn

Annex B

What is the GFF?

The Global Futures Forum (GFF) is a multinational community initiated in 2005 that works at the unclassified level to make sense of emerging and future transnational and global security challenges. Its primary goal is to foster the development of enhanced insight and foresight among its membership through the exchange of diverse perspectives and through the utilisation of collaborative analytic tools.

Who is the GFF?

GFF seeks to involve a diverse population of governmental and private sector subject matter experts to stimulate cross-cultural and interdisciplinary thinking and to challenge prevailing assumptions. Membership in the GFF is limited to governmental intelligence organisations and other governmental organisations focused on foreign, internal, or international security issues. All such organisations regularly seek to monitor, understand, and forecast threats to national and international security as either their main line of work or as an ancillary function to policy formation or operations. GFF participants include analysts from intelligence, diplomatic, defence, and homeland security agencies, along with counterparts from academia, non-government organisations, and industry. More than 1,500 officials and experts from over 50 countries have taken part in GFF activities to date.

Argentina	**EUROPOL ****	**Lithuania**	**Slovakia**
Australia *	**Finland ***	**Luxemburg**	**South Africa**
Austria **	**France ***	**Malaysia**	**South Korea**
Bangladesh	**Germany**	**Mexico ***	**Spain ***
Belgium *	**Greece**	**New Zealand**	**Sweden ***
Brazil	**Hungary ***	**Norway**	**Switzerland ***
Brunei	**India**	**Panama**	**The Netherlands ***
Bulgaria	**Indonesia**	**Philippines**	**Turkey**
Cambodia	**Ireland**	**Poland ***	**United Arab Emirates**
Canada *	**Israel**	**Portugal ***	**United Kingdom ***
Chile	**Italy ***	**Romania ***	**United States ***
Czech Republic *	**Japan ***	**Singapore ***	**Vietnam**
Denmark *	**Jordan**		**** Members***
Estonia	**Latvia ***		***** Observer***

How does the GFF work?

General meetings every two years: Washington (November 2005); Prague (December 2006); Vancouver (April 2008); Singapore (September 2010); Washington DC (November 2012).

Community of interest (COI) workshops and other events:

Topic-specific meetings held regularly in various member countries.

What are the GFF COIs?

At present, the seven COIs focus respectively on:

- Emerging and disruptive technologies
- Human and natural resource security
- Illicit trafficking
- Practice and organisation of intelligence
- Understanding violent extremism
- Proliferation
- Strategic foresight and warning

Annex C

Academic Outreach at CSIS

Intelligence in a shifting world

It has become a truism to say that the world today is changing at an ever faster pace. Analysts, commentators, researchers and citizens from all backgrounds—in and outside government—may well recognise the value of this cliché, but most are only beginning to appreciate the very tangible implications of what otherwise remains an abstract statement.

The global security environment, which refers to the various threats to geopolitical, regional and national stability and prosperity, has changed profoundly since the fall of Communism, marking the end of a bipolar world organised around the ambitions of, and military tensions between, the United States and the former USSR. Quickly dispelling the tempting end of history theory of the 1990s, the 2001 terrorist attacks on the United States, as well as subsequent events of a related nature in different countries, have since further affected our understanding of security.

Globalisation, the rapid development of technology and the associated sophistication of information and communications have influenced the work and nature of governments, including intelligence services. In addition to traditional state-to-state conflict, there now exist a wide array of security challenges that cross national boundaries, involve non-state actors and sometimes even non-human factors. Those range from terrorism, illicit networks and global diseases to energy security, international competition for resources, and the security consequences of a deteriorating natural environment globally. The elements of national and global security have therefore grown more complex and increasingly interdependent.

What we do

It is to understand those current and emerging issues that CSIS launched, in September 2008, its academic outreach program. By drawing regularly on knowledge from experts and taking a multidisciplinary, collaborative approach in doing so, the Service plays an active role in fostering a contextual understanding of security issues for the benefit of its own experts, as well as the researchers and specialists we engage. Our activities aim to shed light on current security issues, to develop a

long-term view of various security trends and problems, to challenge our own assumptions and cultural bias, as well as to sharpen our research and analytical capacities.

To do so, we aim to:

- tap into networks of experts from various disciplines and sectors, including government, think-tanks, research institutes, universities, private business and non-governmental organisations (NGOs) in Canada and abroad. Where those networks do not exist, we may create them in partnership with various organisations;

- stimulate the study of issues related to Canadian security and the country's security and intelligence apparatus, while contributing to an informed public discussion about the history, function and future of intelligence in Canada.

The Service's academic outreach program resorts to a number of vehicles. It supports, designs, plans and/or hosts several activities, including conferences, seminars, presentations and round-table discussions. It also contributes actively to the development of the Global Futures Forum, a multinational security and intelligence community which it has supported since 2005.

While the academic outreach program does not take positions on particular issues, the results of some of its activities are released on the CSIS web site (www.csis-scrs.gc.ca). By publicising the ideas emerging from its activities, the program seeks to stimulate debate and encourage the flow of views and perspectives between the Service, organisations and individual thinkers.